(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: **US 2016/0337325 A1**
BLOMQVIST (43) Pub. Date: **Nov. 17, 2016**

(54) **KEY MANAGEMENT**

(71) Applicant: **NOKIA TECHNOLOGIES**, Espoo (FI)

(72) Inventor: **Kim BLOMQVIST**, Espoo (FI)

(73) Assignee: **NOKIA CORPORATION**, Espoo (FI)

(21) Appl. No.: **15/112,376**

(22) PCT Filed: **Feb. 18, 2014**

(86) PCT No.: **PCT/FI2014/050118**
§ 371 (c)(1),
(2) Date: **Jul. 18, 2016**

Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(52) **U.S. Cl.**
CPC *H04L 63/061* (2013.01); *H04L 63/166* (2013.01); *H04L 63/0435* (2013.01); *H04L 9/3247* (2013.01); *H04L 63/0272* (2013.01)

(57) **ABSTRACT**

According to an example embodiment of the present invention there is provided an apparatus comprising a receiver configured to receive a pair of cryptographic keys comprising a public key and a secret key, the public key being cryptographically signed, a memory configured to store the secret key, and a transmitter configured to send the cryptographically signed public key to a correspondent node and participate in establishment of a cryptographic network protocol session based at least in part on the pair of cryptographic keys.

510
Receiving a pair of cryptographic keys comprising a public key and a secret key, the public key being cryptographically signed

520
Storing the secret key

530
Sending the public key to a correspondent node and participating in establishment of a cryptographic network protocol session based at least in part on the pair of cryptographic keys